

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

10/13/2011

**SUBJECT:**

Multiple Vulnerabilities in Apple Mac OS X and Apple Safari Could Allow Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Apple Mac OS X and Apple Safari that could allow remote code execution. Apple Mac OS X is a desktop operating system for the Apple Mac. Apple Safari is a web browser available for Mac OS X and Microsoft Windows. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, using a vulnerable version of Apple Mac OS X or Apple Safari. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**SYSTEMS AFFECTED:**

- Apple OS X 10.7.1 and earlier
- Apple Safari 5.1 and earlier

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users:** **High**

**DESCRIPTION:**

Multiple vulnerabilities have been discovered in Apple Mac OS X and Apple Safari that could allow both remote and local code execution. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, with a vulnerable version of Apple Mac OS X or Apple Safari.

Apple has identified the following vulnerabilities:

- A remote format-string vulnerability affects the debug logging of the Application Firewall because it fails to properly sanitize user-supplied input before including it in the format-specifier argument of a formatted-printing function. Attackers can execute arbitrary code with elevated privileges by executing a binary with a specially crafted name.

- A memory-corruption issue occurs in the ATS application because of a signedness error when handling specially crafted Type 1 fonts. Attackers can execute arbitrary code on the victim's system by sending a document which contains a maliciously crafted embedded font.
- A memory-corruption issue occurs in the ATS application because of an out-of-bounds memory access when handling specially crafted Type 1 fonts. Attackers can execute arbitrary code in the victim's system by sending a document which contains a maliciously crafted embedded font.
- A buffer-overflow issue affects applications which use 'ATSFontDeactivate' API because it fails to properly bounds-check user-supplied input.
- A vulnerability affects the CFNetwork component because of a synchronization error when handling the cookie policies. This allows attackers to store cookies in the Safari browser against the configured preferences.
- A cross-domain information-disclosure vulnerability affects the CFNetwork component because it fails to enforce the same-origin policy. This issue occurs due to an error in handling of HTTP cookies when accessing a maliciously crafted HTTP or HTTPS URL. Attackers can exploit this issue to obtain sensitive cookie information of another domain by enticing a victim to visit a maliciously crafted website.
- Multiple memory-corruption issues affect the CoreMedia component when handling specially crafted QuickTime movie files.
- A local security-bypass issue affects the CoreProcesses component, which allows attackers to partially bypass the screen lock.
- An information-disclosure issue affects the CoreStorage component because it fails to erase all existing data, when converting to FileVault.
- An information-disclosure issue affects the application because it allows attackers to manipulate HTTPS server certificates by performing man-in-the-middle attacks. This issue occurs when handling WebDAV volumes on HTTPS servers.
- A local security-bypass issue affects the IOGraphics component, which allows attackers to bypass the screen lock without entering a password, when the system is in display sleep mode.
- A local information-disclosure issue occurs because of a logic error in the kernel's DMA protection. This issue allows local attackers to access the user's password.
- A local security-bypass issue occurs because of a logic error in the kernel's handling of file deletions in directories with the sticky bit. This allows an unprivileged attacker to delete another user's files in a shared directory.
- Multiple memory-corruption issues affect the MediaKit component when handling specially crafted disk images.
- A local information-disclosure issue affects the Open Directory application because of an access control error. This allows local attackers to read another user's password data.
- A local security-bypass issue affects the Open Directory application because of an access control error. This allows local authenticated attackers to change the account's password without providing the current password.
- A local security-bypass issue affects the Open Directory application when it is bound to an LDAPv3 server using RFC2307 or custom mappings.
- Multiple memory-corruption issues affect the QuickTime player when handling the specially crafted movie files.
- A cross-site scripting issue exists in QuickTime player's 'Save for Web' export feature. This issue occurs because template HTML files generated by this feature references a script file from

a non-encrypted origin. Attackers can perform man-in-the-middle attacks to inject script in the local domain which executes when viewing the template HTML.

- A memory-corruption issue affects the QuickTime Player because of an uninitialized memory access error when handling URL data handlers within specially crafted movie files.
- A remote-code execution issue affects the QuickTime Player when handling the atom hierarchy within a specially crafted movie file.
- A buffer overflow issue affects the QuickTime Player when handling the FlashPix files.
- A buffer overflow issue affects the QuickTime Player when handling the FLIC files.
- A security-bypass issue affects the SMB File Server because of an access control error, which allows guest users to browse shared folders.
- A security-bypass issue occurs when App Store help content is updated over HTTP. Attackers can perform man-in-the-middle attacks to manipulate App Store help content, which may also lead to arbitrary code execution.
- A vulnerability resulting in remote-code execution affects the 'libsecurity' library because of an error handling issue which occurs when parsing a nonstandard certificate revocation list extension.
- A directory traversal issue exists during the handling of 'safari-extension://' URLs. An attacker can exploit this issue to execute arbitrary script-code in the browser.
- A remote code-execution vulnerability exists due to a policy issue when handling 'file://' URLs.
- A remote code-execution vulnerability occurs when handling certain SSL certificates.
- An issue regarding in 'Private Browsing' mode that may allow cookies to be set regardless of the 'Block cookies' setting.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed attempts could result in a denial-of-service.

## **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Apple to affected systems immediately after appropriate testing.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Permit local access for trusted individuals only. Where possible, use restricted environments and restricted shells.

## **REFERENCES:**

### **Apple:**

<http://support.apple.com/kb/HT5002>  
<http://support.apple.com/kb/HT5002>

<http://support.apple.com/kb/HT5000>  
<http://support.apple.com/kb/HT5000>

### **SecurityFocus:**

<http://www.securityfocus.com/advisories/23106>  
<http://www.securityfocus.com/advisories/23106>

<http://www.securityfocus.com/advisories/23109>  
<http://www.securityfocus.com/advisories/23109>

### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0185>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0185>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0224>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0224>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0229>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0229>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0230>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0230>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0231>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0231>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0246>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0246>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0247>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0247>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0248>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0248>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3214>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3214>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3215>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3215>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3216>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3217>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3218>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3220>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3221>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3222>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3223>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3224>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3225>

[http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3226](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0246)

[http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3227](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0247)

[http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3228](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0248)

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3246>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3435>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3436>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3437>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3229>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3230>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3231>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3242>